Remarks

In the present response, five claims (1, 2, 11, 15, and 16) are amended, and seven claims (20-26) are newly submitted. Applicants believe that no new matter is entered.

I. Drawings

Formal drawings are included herewith. Further, the drawings of FIGS. 1 and 2 are amended to include the reference numeral 20 as mentioned in the description. No new matter is entered.

II. Specification

The Specification is amended at page 12, lines 9-14 and at page 14, lines 5-10. No new mater is entered.

III. Claim Objections

Claim 1 is amended to correct a typographical error. Specifically, the word "in" is changed to "is".

IV. Claims Rejection (Claims 1-5, 11, 14-15, and 17-19) – 35 USC § 102(e)

Claims 1-5, 11, 14-15, and 17-19 are rejected under 35 USC § 102(e) as being anticipated by Baker et al. (USPN 6,611,498, hereinafter "Baker").

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See MPEP § 2131, also, *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

Claim 1

Claim 1 is rejected under 35 U.S.C. §102 as allegedly anticipated by Baker. Claim 1 is currently amended and reads as follows (emphasis added):

A method for securely transferring data between an agent and an application server through a non-secure node comprising:

(a) establishing a session key between the agent and the application server by utilizing a public key of the application server; **wherein the public key of the**

application server is embedded in the agent to enable the agent to derive the session key; and

(b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non -secure node by using a relay module.

Claim 1 recites numerous limitations that are not taught in Baker. For example, claim 1 recites that "the public key of the application server is embedded in the agent to enable the agent to derive the session key." This limitation is not taught in Baker. By contrast, Baker teaches a "cookie" that is sent to the client and then returned to the server. Specifically, Baker teaches:

> The preferred embodiment further associates a given HTTPS request with a logical session which is initiated and tracked by a "cookie jar server" 28 to generate a "cookie" which is a unique server-generated key that is sent to the client along with each reply to a HTTPS request. The client holds the cookie and returns it to the server as part of each subsequent HTTPS request. (Col. 9, lines 7-13)

Claim 1 recites that the public key is embedded in the agent **to enable the agent to derive the session key**. In Baker, the "cookie" is not embedded in the agent to enable the cookie to derive a session key. Rather, the cookie is sent to the client and returned to the server.

Thus, the cited art does not teach or suggest each and every limitation of claim 1. Claims 2-5 depend from independent claim 1 and, hence, inherit all limitations of the base claim. Accordingly, claim 2-5 are allowable over Baker.

Claim 11

Claim 11 is rejected under 35 U.S.C. §102 as allegedly anticipated by Baker. Claim 11 is currently amended and reads as follows (emphasis added):

The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising:

a) a user accessing the web -server to download the agent therefrom; **wherein the agent includes a public key of the application server;**

b) **the agent deriving a shared session key with the application server by using the public key of the application server**, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server;

c) the application server establishing a connection to the web-server; and

d) the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server.

Claim 11 recites numerous limitations that are not taught in Baker. For example, claim 11 recites that "the agent includes a public key of the application server." This limitation is not disclosed in Baker. The Examiner cites Baker (Col. 11, lines 34-38) to teach utilizing a public key and then cites Baker (Col. 9, lines 10-12) to teach an agent including a public key. Applicants respectfully disagree. Baker (Col. 11, lines 34-38) teaches public key encryption, such as employed by a secure sockets layer (SSL). Baker (Col 9, lines 10-12) teaches a server to generate a "cookie" that is sent to the client. A "cookie" is **not** a public key. These two terms have entirely different meanings to one of ordinary skill in the art. Per Webopedia (see www.webopedia.com), a cookie is defined as "A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server." By contrast, a public key is defined as "A cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message." Thus, these sections taken together do not teach an "agent that includes a public key of the application server."

Claim 11 also recites that the agent derives a shared session key with the application sever by using the public key of the application server. This limitation is not taught in Baker. Applicants reproduce the cited sections of Baker:

> When a client logs onto the web server 632 and is authenticated, the client is provided a "session id" which is a unique server-generated key. The client holds this and returns it to the server as part of subsequent message transaction. (Col. 17, lines 6-10).

Note the difference between the recitations of claim 11 and the teachings of this section. Claim 11 recites that the agent **derives** the shared session key. The cited section of Baker teaches a client that is provided with a session id. In Baker, the client does not "derive" the session id.

Thus, the cited art does not teach or suggest each and every limitation of claim 11. Claim 14 depends from independent claim 11 and, hence, inherits all limitations of the base claim. Accordingly, claim 14 is allowable over Baker.

Claim 15

Claim 15 is rejected under 35 U.S.C. §102 as allegedly anticipated by Baker. Claim 15 as amended reads as follows (emphasis added):

A secure data transfer system for connecting a non -secure node to an application server behind a firewall comprising:

a) a web-server in the non-secure node;

b) a relay in the non-secure node that is dynamically instantiated by the application server, **the relay being configured by the application server to have a first port for listening for a connection from the application server**;

wherein the application server connects to the relay on the first port and reads data from the first port.

Claim 15 recites numerous limitations that are not taught in Baker. For example, claim 15 recites that the relay is "configured by the application server." This limitation is not taught in Baker. Further, the claim recites that the relay is configured by the application server to have "a first port for listening for a connection from the application server." This limitation is not taught in Baker.

The Examiner cites Baker (Col. 16, lines 3-5). This section is reproduced below:

> The HTTP service manager 652 spawns a process to run an instance of the message manager 656 each time it receives a message transaction from the client.

As is evident, this section does not teach the recited limitation of claim 15: "the relay being configured by the application server to have a first port for listening for a connection from the application server."

Claim 17

Claim 17 is rejected under 35 U.S.C. §102 as allegedly anticipated by Baker. Claim 17 reads as follows (emphasis added):

A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node comprising:

a) a web-server residing in the non-secure node, **the web-server having the agent that includes a public key of the application server**;

b) a browser in communication with the web-server for downloading the agent from the web-server;

c) a secure transfer module residing in the non-secure node; and

d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

Claim 17 recites numerous limitations that are not taught in Baker. For example, claim 17 recites: "the web-server having the agent that includes a public key of the application server." The Examiner cites Baker (Col. 9, lines 10-12) as teaching this recitation. Specifically, Baker teaches:

> The preferred embodiment further associates a given HTTPS request with a logical session which is initiated and tracked by a "cookie jar server" 28 to generate a "cookie" which is a unique server-generated key that is sent to the client along with each reply to a HTTPS request. The client holds the cookie and returns it to the server as part of each subsequent HTTPS request. (Col. 9, lines 7-13)

This section teaches a server 28 that generates a "cookie" that is sent to a client. First, as noted herein, a "cookie" is **not** a public key. Secondly, the bolded section of claim 17 recites four different elements: (1) a web-server, (2) an agent, (3) a public key, and (4) an application server. The portion of Baker cited by the Examiner does not even include four different elements. Applicants respectfully ask the Examiner to specify the portions of Baker that correspond with the elements of claim 17.

Thus, the cited art does not teach or suggest each and every limitation of claim 17. Claims 18-19 depend from independent claim 17 and, hence, inherit all limitations of the base claim. Accordingly, claims 18-19 are allowable over Baker.

V. Claims Rejection (Claims 6-8) – 35 USC § 103(a)

Claims 6-8 are rejected under 35 USC §103(a) as being unpatentable over Baker in view of Cury et al. (USPN 6,237,095). Claims 6-8 depend from claim 1 and, hence, inherit all the limitations of the base claim. Since Cury does not cure the deficiencies of Baker, claims 6-8 are allowable over the combination of Baker and Cury.

VI. Claims Rejection (Claims 9-10) – 35 USC § 103(a)

Claims 9-10 are rejected under 35 USC §103(a) as being unpatentable over Baker in view of Boyle et al. (USPN 6,119,167). Claims 9-10 depend from claim 1 and, hence, inherit all the limitations of the base claim. Since Boyle does not cure the deficiencies of Baker, claims 9-10 are allowable over the combination of Baker and Boyle.

VII. Claims Rejection (Claims 12 and 16) – 35 USC § 103(a)

Claims 12 and 16 are rejected under 35 USC §103(a) as being unpatentable over Baker in view of Bradley et al. (USPN 6,584,507). Claim 12 depends from claim 11, and claim 16 depends from claim 15. Claims 12 and 16 inherit all the limitations of the respective base claim. Since Bradley does not cure the deficiencies of Baker, claims 12 and 16 are allowable over the combination of Baker and Bradley.

VIII. Claim Rejection (Claim 13) – 35 USC § 103(a)

Claim 13 is rejected under 35 USC §103(a) as being unpatentable over Baker in view of Bradley and Cury. Claim 13 depends from claim 11 and, hence, inherits all the limitations of the base claim. Since Bradley and Cury do not cure the deficiencies of Baker, claim 13 is allowable over the combination of Baker, Bradley, and Cury.

IX. New Claims (20-26)

Applicants submit new claims 20-26. These claims have numerous recitations that are not shown or suggested in the art of record.

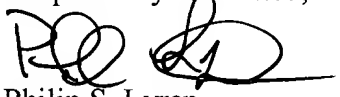
CONCLUSION

In view of the above, Applicant believes claims 1-26 are in condition for allowance. Allowance of these claims is respectfully requested.

Any inquiry regarding this Amendment and Response should be directed to Philip S. Lyren at Telephone No. (281) 514-8236, Facsimile No. (281) 514-8332. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,



Philip S. Lyren
Reg. No. 40,709
Ph: 281-514-8236

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 21st day of April, 2004.

By Be Henry
Name: Be Henry